**Introducción**

Los administradores de Azure necesitan proteger el acceso a sus recursos de Azure, como máquinas virtuales (VM), sitios web, redes y almacenamiento. Los administradores necesitan mecanismos para ayudarles a administrar quién puede acceder a sus recursos y qué acciones se permiten. Las organizaciones que hacen negocios en la nube reconocen que proteger sus recursos es una función crítica de su infraestructura.

En este módulo, su empresa está investigando cómo asegurarse de que sus datos y recursos corporativos están protegidos. Quieren una protección segura que les permita controlar el acceso a sus datos y recursos mediante la especificación de roles y privilegios de acceso para empleados y asociados comerciales. Es responsable de investigar cómo usar el control de acceso basado en rol (RBAC) para realizar estas tareas. Debe asegurarse de que los recursos de la empresa están protegidos y también admitir el acceso de los usuarios a los recursos.

El objetivo de este módulo es comprender las características y los casos de uso del control de acceso basado en roles (RBAC) de Azure. Ha descubierto cómo crear definiciones de roles y asignaciones de roles, y buscar y usar roles RBAC de Azure integrados. Además, explorará cómo usar RBAC para administrar el acceso a las suscripciones. También revisará las diferencias entre los roles RBAC de Azure y Entra ID.

**Objetivos de aprendizaje**

En este módulo aprenderá a:

* Conocer los conceptos y principios de RBAC de Azure.
* Crear definiciones de roles y asignaciones de roles.
* Identifique las diferencias entre los roles RBAC de Azure y Microsoft Entra.
* Usar RBAC para administrar el acceso a los recursos.
* Revisar y seleccionar el mejor rol integrado de Azure para un escenario.

**Requisitos previos**

* Conocimientos de Azure. Tener un conocimiento general de los servicios, conceptos y terminología de Azure que le ayude a comprender RBAC de forma más eficaz.
* Conceptos de identidad. Un conocimiento básico de Microsoft Entra ID, que es el servicio de administración de identidades y acceso basado en la nube de Microsoft, es esencial. Los conocimientos de conceptos como usuarios, grupos, roles y permisos son útiles.
* Administración de recursos de Azure. Comprender cómo se organizan, implementan y administran los recursos proporciona contexto para la implementación de RBAC.
* Modelos de control de acceso. Conocimiento de los modelos de control de acceso, como el control de acceso discrecional (DAC) y el control de acceso obligatorio (MAC). Este conocimiento le ayuda a comprender los principios subyacentes a RBAC y sus ventajas sobre los mecanismos de control de acceso tradicionales.

**Implementación del control de acceso basado en roles**

La administración de acceso seguro para los recursos en la nube es fundamental para las empresas que operan en la nube. El control de acceso basado en rol (RBAC) es un mecanismo que puede ayudarle a administrar quién puede acceder a los recursos de Azure. RBAC le permite determinar qué operaciones pueden hacer los usuarios específicos en recursos específicos y controlar a qué áreas de un recurso puede tener acceso cada usuario.

RBAC es un sistema de autorización basado en Azure Resource Manager. El RBAC permite una administración de acceso muy detallado de los recursos en Azure.

**Aspectos que debe saber sobre RBAC de Azure**

Estas son algunas cosas que puede realizar con RBAC de Azure:

* Permitir que una aplicación acceda a todos los recursos de un grupo de recursos.
* Permitir que un usuario administre las VM en una suscripción y que otro usuario administre las redes virtuales.
* Permitir a un grupo de administradores de base de datos (DBA) administrar bases de datos SQL en una suscripción.
* Permitir que un usuario administre todos los recursos de un grupo de recursos, como las máquinas virtuales, los sitios web y las subredes.

**Conceptos de RBAC de Azure**

En la tabla siguiente se describen los conceptos básicos de RBAC de Azure.

| **Concepto** | **Descripción** | **Ejemplos** |
| --- | --- | --- |
| **Entidad de seguridad** | Objeto que representa un elemento que solicita acceso a los recursos. | Usuario, grupo, entidad de servicio o identidad administrada |
| **Definición de roles** | Conjunto de permisos que enumera las operaciones permitidas. RBAC de Azure incluye definiciones de roles integradas, pero también puede crear sus propias definiciones de roles personalizados. | Algunas definiciones de roles integradas: *Lector*, *Colaborador*, *Propietario*, *Administrador de acceso de usuario* |
| **Ámbito** | Límite del *nivel* de acceso solicitado o "cuánto" se concede. | Grupo de administración, suscripción, grupo de recursos, recurso |
| **Cesión** | Una **asignación** añade una **definición de roles** a una **entidad de seguridad**en un ámbito **determinado**. Los usuarios pueden conceder el acceso descrito en una definición de roles mediante la creación (adición) de una asignación al rol. | - Asignar el rol *Administrador de acceso de usuario* a un grupo de administración con ámbito a un grupo de administración - Asignar el rol *Colaborador* a un usuario con ámbito a una suscripción |

**Aspectos que se deben tener en cuenta al usar RBAC de Azure**

A medida que piense en cómo puede implementar roles y asignaciones de ámbito dentro de su organización, tenga en cuenta estos puntos:

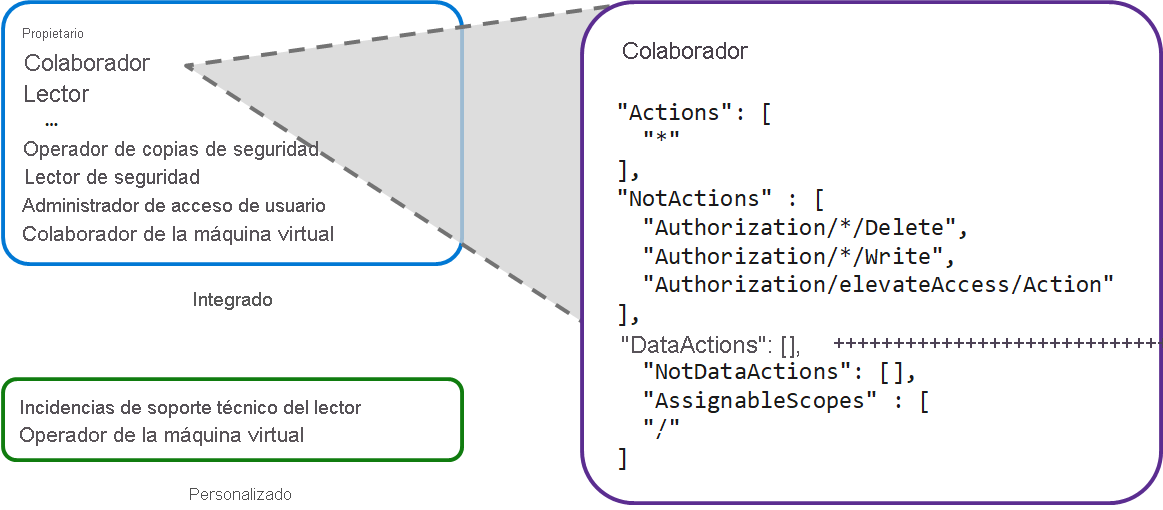
* **Tenga en cuenta los solicitantes**. Planee su estrategia para adaptarse a todos los tipos de acceso a los recursos. Las entidades de seguridad se crean para todo lo que solicite acceso a los recursos. Determine quiénes son los solicitantes de su organización. Los solicitantes pueden ser usuarios internos o externos, grupos de usuarios, aplicaciones y servicios, recursos, etc.
* **Tenga en cuenta sus roles**. Examine los tipos de responsabilidades de trabajo y los escenarios de trabajo de su organización. Los roles se suelen crear en torno a los requisitos para cumplir las tareas de trabajo o completar los objetivos de trabajo. Algunos usuarios, como administradores, controladores corporativos e ingenieros, pueden requerir un nivel de acceso más allá de lo que la mayoría de los usuarios necesitan. Algunos roles se pueden definir para proporcionar el mismo acceso a todos los miembros de un equipo o departamento para recursos o aplicaciones específicos.
* **Considere el ámbito de los permisos**. Piense en cómo puede garantizar la seguridad controlando el ámbito de los permisos para las asignaciones de roles. Describa los tipos de permisos y niveles de ámbito que necesita admitir. Puede aplicar distintos niveles de ámbito para un único rol para admitir solicitantes en distintos escenarios.
* **Considere las definiciones integradas o personalizadas**. Revise la lista de definiciones de roles integrado en el RBAC de Azure. Los roles integrados se pueden usar tal y como están o ajustados para satisfacer los requisitos específicos de su organización. También puede crear definiciones de rol personalizadas desde cero.

**Creación de una definición de roles**

Una definición de rol consta de un conjunto de permisos definidos en un fichero JSON. Cada conjunto de permisos tiene un nombre, como *Actions* o *NotActions*, que describe los permisos. Algunos ejemplos de conjunto de permisos son:

* Los permisos *Actions* especifican qué acciones se permiten.
* Los permisos*NotActions* especifican qué acciones no se permiten.
* Los permisos*DataActions* indican cómo se pueden modificar o usar los datos.
* Los permisos*AssignableScopes* enumeran los ámbitos en los que se puede asignar una definición de rol.

En el diagrama siguiente se muestran los detalles del rol *Contributor* en el RBAC de Azure.



Los permisos *Actions* indican que el rol *Colaborador* tiene todos los privilegios de acción. El comodín (carácter asterisco "\*") significa "todo". Los permisos *NotActions* acotan los privilegios que proporciona el conjunto de acciones *Actions* y prohíben tres acciones:

* Authorization/\*/Delete: No está autorizado a eliminar o quitar en "todo".
* Authorization/\*/Write: No está autorizado a escribir o cambiar en "todo".
* Authorization/elevateAccess/Action: No está autorizado a subir el nivel o el ámbito de los privilegios de acceso.

El rol *Contributor* también tiene dos permisos que especifican cómo pueden verse afectados los datos:

* "NotDataActions": []: No se enumera ninguna acción concreta. Por tanto, todas las acciones podrán afectar a los datos.
* "AssignableScopes": ["/"]: El rol se puede asignar a todos los ámbitos que afecten a los datos.

**Lo que hay que saber sobre las definiciones de roles**

Revise las siguientes características de las definiciones de roles:

* El RBAC de Azure proporciona roles y conjuntos de permisos integrados. También se pueden crear permisos y role personalizados.
* El rol integrado *Propietario* tiene el nivel más alto de privilegios de acceso en Azure.
* El sistema resta los permisos *NotActions* de los permisos *Actions* para determinar los *permisos efectivos* de un rol.
* Los permisos *AssignableScopes* de un rol pueden ser grupos de administración, suscripciones, grupos de recursos o recursos.

**Permisos de los roles**

Combine los permisos *Actions* y *NotActions* para conceder y denegar los privilegios exactos a cada rol. Los permisos *Actions* pueden dar amplitud de acceso, mientras que los permisos *NotActions* pueden acotar el acceso.

La tabla siguiente muestra cómo se usan los permisos *Actions* y *NotActions* en las definiciones de tres roles integrados: *Propietario*, *Colaborador* y *Lector*. Los permisos se van acotando desde el rol *Propietario* a los roles *Colaborador* y *Lector* para restringir el acceso.

| **Nombre de rol** | **Descripción** | **Permisos de Actions** | **Permisos de NotActions** |
| --- | --- | --- | --- |
| *Propietario* | Permitir todas las acciones | \* | N/D |
| *Colaborador* | Permitir todas las acciones menos la asignación de los roles de escritura o borrado | \* | - Microsoft.Authorization/\*/Delete - Microsoft.Authorization/\*/Write - Microsoft.Authorization/elevateAccess/Action |
| *Lector* | Permitir todas las acciones de lectura | /\*/read | N/D |

**Ámbitos de rol**

Una vez definidos los permisos de un rol, use los permisos *AssignableScopes* para especificar cómo se puede asignar dicho rol. Veamos algunos ejemplos.

* Dé a un rol el ámbito de disponible para su asignación en dos suscripciones:

"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e", "/subscriptions/e91d47c4-76f3-4271-a796-21b4ecfe3624"

* Dé a un rol el ámbito de disponible para su asignación solo en el grupo de recursos de Red:

"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups/Network"

* Dé a un rol el ámbito de disponible para su asignación a todos los solicitantes:

"/"

**Aspectos que hay que tener en cuenta al crear roles**

Tenga en cuenta los siguientes puntos relativos a la creación de definiciones de rol en el RBAC de Azure:

* **Considere la posibilidad de usar roles integrados**. Consulte la lista de [definiciones de roles integrados](https://learn.microsoft.com/es-es/azure/role-based-access-control/built-in-roles) en el RBAC de Azure. Hay más de 100 definiciones de roles predefinidos entre las que elegir, como, por ejemplo, *Owner*, *Backup Operator*, *Website Contributor* y *SQL Security Manager*. Los roles integrados se definen para varias categorías de servicios, tareas y usuarios como, por ejemplo, General, Redes, Almacenamiento, Bases de datos, etc.
* **Considere la posibilidad de crear definiciones personalizadas**. Defina sus propios [roles personalizados](https://learn.microsoft.com/es-es/azure/role-based-access-control/custom-roles) que respondan a escenarios de negocio específicos de su organización. Puede modificar los permisos de un rol integrado para que se adapte a las necesidades específicas de su organización. También puede crear definiciones de rol personalizadas desde cero.
* **Considere la posibilidad de limitar el ámbito de acceso**. Asigne los roles con el nivel mínimo de ámbito necesario para realizar las tareas necesarias. Algunos usuarios como, por ejemplo, los administradores, requieren acceso total a los recursos corporativos para mantener la infraestructura. Otros usuarios de la organización pueden requerir acceso de escritura a recursos personales o del equipo, y acceso de solo lectura a los recursos compartidos de la empresa.
* **Considere la posibilidad de controlar los cambios en los datos**. Identifique los datos o recursos que solo se deben modificar en determinados escenarios y aplique un estricto control de acceso. Restrinja el acceso de los usuarios al mínimo necesario para que puedan hacer su trabajo. Una estrategia de administración de acceso bien planeada ayuda a mantener la infraestructura y a evitar problemas de seguridad.
* **Considere la posibilidad de aplicar asignaciones de denegación**. Determine si necesita implementar la característica de asignación de denegación. De forma similar a una asignación de roles, una asignación de denegación asocia un conjunto de acciones de denegación a un usuario, grupo o entidad de servicio en un ámbito determinado con el fin de denegar el acceso. Las asignaciones de denegación impiden que los usuarios realicen acciones concretas en recursos de Azure, aunque una asignación de roles les conceda acceso.

**Crear una asignación de rol**

Una asignación de roles es el proceso de establecer el ámbito de una definición de roles para limitar permisos a un usuario, un grupo, una entidad de servicio o identidad administrada.

**Lo que hay que saber sobre las definiciones de roles**

Revise las siguientes características de las definiciones de roles:

* El propósito de la asignación de roles es conceder acceso.
* Los límites de ámbito que se definen para un rol están disponibles para el solicitante asignado.
* El acceso se revoca quitando una asignación de roles.
* Un recurso hereda las asignaciones de roles de su recurso principal.
* Los permisos efectivos para un solicitante son una combinación de los permisos para los roles asignados del solicitante y los permisos de los roles asignados a los recursos solicitados.

**Aspectos que se deben tener en cuenta al asignar niveles de ámbito para roles**

En el diagrama siguiente se muestra un ejemplo de cómo se pueden aplicar ámbitos a un rol para conceder distintos niveles de acceso para distintos usuarios. Piense en cómo puede implementar ámbitos para los roles con el fin de crear asignaciones significativas para su organización.



Este escenario tiene la siguiente configuración de administración de acceso:

* Se admiten tres entidades de seguridad: usuario, grupo y entidad de servicio.
* Se implementan seis roles integrados y se definen dos roles personalizados: *Vales de soporte técnico del lector* y *Operador de máquina virtual*.
* El rol *Colaborador* integrado tiene dos conjuntos de permisos: *Actions* y *NotActions*.
* El rol *Colaborador* se asigna en distintos ámbitos al grupo marketing y al grupo de recursos de ventas farmacéuticas:
  + Los usuarios del grupo de marketing pueden crear o administrar cualquier recurso de Azure del grupo de recursos de ventas farmacéuticas.
  + A los usuarios de marketing no se les concede acceso a los recursos fuera del grupo de recursos de ventas farmacéuticas, a menos que tengan otra asignación de roles que les conceda acceso al grupo de recursos.

**Comparación de roles de Azure con roles de Microsoft Entra**

Hay tres tipos de roles disponibles para la administración de acceso en Azure:

* Roles de administrador de suscripciones clásicas
* Roles de control de acceso basado en rol (RBAC) de Azure
* Roles de administrador de Microsoft Entra

Para comprender mejor cómo se definen e implementan estos distintos roles en Azure, ayuda a conocer parte del historial.

Cuando se publicó inicialmente Azure, el acceso a los recursos se administraba con solo tres roles de administrador: *administrador de cuentas*, *administrador de servicios* y *coadministrador*. El acceso se controló mediante la asignación de roles de administrador a suscripciones.

Más adelante, se agregó el control de acceso basado en rol (RBAC) para los recursos de Azure. RBAC de Azure es un nuevo sistema de autorización que proporciona una administración de acceso detallada a los recursos de Azure. RBAC incluye muchos roles integrados que se pueden asignar en distintos ámbitos. El modelo RBAC de Azure también le permite crear sus propios roles personalizados.

Además de los roles de RBAC de Azure, Microsoft Entra ID proporciona roles de administrador integrados para administrar recursos de Microsoft Entra, como usuarios, grupos y dominios.

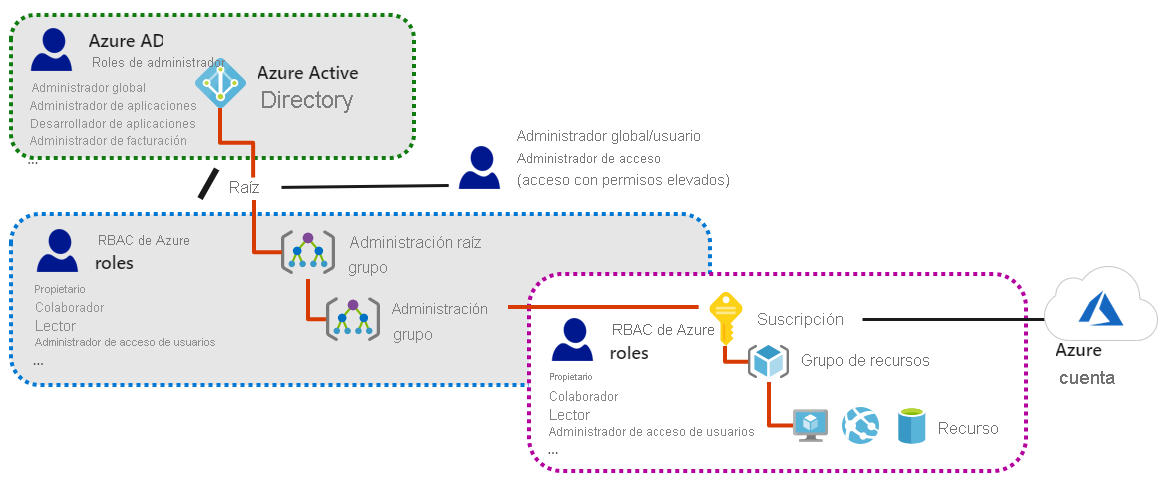
|  | **Roles de RBAC de Azure** | **Roles de administrador de Microsoft Entra ID** |
| --- | --- | --- |
| **Administración de acceso** | Administra el acceso a los recursos de Azure | Administra el acceso a los recursos de Microsoft Entra |
| **Asignación de ámbito** | El ámbito se puede especificar en varios niveles, incluidos los grupos de administración, las suscripciones, los grupos de recursos y los recursos | El ámbito está especificado en el nivel de inquilino |
| **Definiciones de roles**: | Los roles se pueden definir a través de la Azure Portal, la CLI de Azure, Azure PowerShell, las plantillas de Azure Resource Manager y la API REST | Los roles se pueden definir a través del portal de administración de Azure, el portal de administración de Microsoft 365 y PowerShell de Microsoft Graph |

**Aplicación del control de acceso basado en roles**

Las definiciones de roles integradas en RBAC de Azure se definen para varias categorías de servicios, tareas y usuarios. Puede asignar roles integrados en distintos ámbitos para admitir varios escenarios y crear roles personalizados a partir de las definiciones base.

Microsoft Entra ID también proporciona roles integrados para administrar recursos en Microsoft Entra ID, incluidos usuarios, grupos y dominios. Microsoft Entra ID ofrece [roles de administrador](https://learn.microsoft.com/es-es/azure/active-directory/roles/permissions-reference) que puede implementar para su organización, como *Administrador global*, *Administrador de aplicaciones* y *Desarrollador de aplicaciones*.

En el diagrama siguiente se muestra cómo puede aplicar roles de administrador de Microsoft Entra y roles de RBAC de Azure en su organización.



* Los **roles de administrador de Microsoft Entra** se usan para administrar recursos en Microsoft Entra ID, como usuarios, grupos y dominios. Estos roles se definen para el inquilino de Microsoft Entra en el nivel raíz de la configuración.
* **Los roles RBAC de Azure** proporcionan administración de acceso más granular para los recursos de Azure. Estos roles se definen para un solicitante o recurso y se pueden aplicar en varios niveles: la raíz, los grupos de administración, las suscripciones, los grupos de recursos o los recursos.

**Revisión de los roles fundamentales de RBAC de Azure**

Azure RBAC proporciona más de 100 definiciones de roles predefinidas. Los roles pueden conceder acceso a los datos de un objeto. Si un usuario tiene acceso para *leer datos* de una cuenta de almacenamiento, podrá leer los blobs o mensajes de esa cuenta de almacenamiento.

En la tabla siguiente se describen cuatro definiciones de roles RBAC de Azure integradas que se consideran fundamentales.

| **Rol fundamental** | **Descripción** |
| --- | --- |
| *Propietario* | El rol *Propietario* tiene acceso total a todos los recursos, incluido el derecho a delegar el acceso a otros usuarios. Al *administrador de servicios* y a los*coadministradores* se les asigna el rol *Propietario* en el ámbito de la suscripción. |
| *Colaborador* | El rol *Colaborador* puede crear y administrar todos los tipos de recursos de Azure. Este rol no puede conceder acceso a otros usuarios. |
| *Lector* | El rol *Lector* puede ver los recursos existentes de Azure. |
| *Administrador de acceso de usuario* | El rol *Administrador de acceso de usuario* puede administrar el acceso de los usuarios a los recursos de Azure. |

**Prueba de conocimientos**

Su empresa ha decidido implementar el control de acceso basado en rol (RBAC) de Azure para proteger sus recursos y administrar el acceso de los usuarios. Está revisando los escenarios para admitir y tiene una lista de problemas para solucionar:

* No todos los usuarios tienen acceso a los mismos recursos. Un nuevo empleado solo debe tener acceso limitado a los recursos.
* La mayoría de los administradores requieren acceso total a todos los recursos corporativos. Algunos administradores necesitan acceso limitado a recursos específicos para que puedan leer la configuración, pero no realizar cambios.
* ¿Cómo se aplican los ámbitos y permisos para los recursos de Azure, incluida la definición de roles personalizados?
* El administrador ha preguntado si hay diferencias entre los roles de Azure y los roles de Microsoft Entra.

**Responda a las siguientes preguntas**

Elija la respuesta más adecuada para cada una de las preguntas siguientes. Después, seleccione **Comprobar las respuestas**.

Principio del formulario

**1. Hay tres máquinas virtuales (VM1, VM2 y VM3) en un grupo de recursos. Se contrata a un nuevo administrador y deben poder modificar la configuración en VM3. No deben poder realizar cambios en VM1 o VM2. ¿Cómo puede implementar RBAC para minimizar la sobrecarga administrativa?**

1. Asignar el usuario al rol Colaborador en el grupo de recursos.
2. Asignar el administrador al rol Colaborador en la VM3.
3. Mover VM3 a un nuevo grupo de recursos y asignar al administrador el rol Propietario en VM3.

**2. ¿Cuál es el propósito de los permisos "AssignableScopes" en una definición de rol?**

1. Especifica las acciones que no están permitidas
2. Especifica los ámbitos en los que se puede asignar una definición de rol
3. Especifica las acciones que no están permitidas

**3. Explicar las principales diferencias entre los roles de Azure y los roles de Microsoft Entra.**

1. Los roles de Azure aplican a los recursos de Azure. Los roles de Microsoft Entra se aplican a recursos de Microsoft Entra, como usuarios, grupos y dominios.
2. Los roles de Azure se pueden asignar en el nivel de raíz.
3. Los roles de Microsoft Entra se usan para administrar el acceso a los recursos de Azure.
4. B
5. B
6. A

Final del formulario

**Resumen y recursos**

El control de acceso basado en rol (RBAC) de Azure es un sistema que permite la administración granular del acceso de los recursos de Azure. Los administradores de Azure usan RBAC de Azure para separar las tareas de un equipo y conceder a los usuarios el acceso específico que necesitan para realizar sus trabajos.

En este módulo, ha identificado las características y los casos de uso de RBAC. Ha descubierto cómo crear definiciones de roles y asignaciones de roles y buscar y usar roles RBAC de Azure integrados. Ha explorado cómo usar RBAC para administrar el acceso a las suscripciones con RBAC. Ha revisado las diferencias entre los roles RBAC de Azure y Microsoft Entra.

Las principales conclusiones de este módulo son:

* Azure RBAC es un sistema que permite la administración de acceso granular de los recursos de Azure. Permite separar las tareas dentro de un equipo y conceder a los usuarios acceso específico en función de sus requisitos de trabajo.
* Las definiciones de roles de Azure RBAC definen conjuntos de permisos que enumeran las operaciones permitidas. Use definiciones de roles integradas o cree definiciones de roles personalizadas para cumplir con los requisitos específicos de su organización.
* Las asignaciones de roles adjuntan definiciones de roles a entidades de seguridad en un ámbito determinado. Esta asignación determina el nivel de acceso concedido al solicitante. El acceso se puede revocar quitando una asignación de roles.
* Los roles RBAC de Azure se pueden asignar a distintos ámbitos, incluyendo los grupos de administración, las suscripciones, los grupos de recursos y los recursos. El ámbito limita los permisos disponibles para el solicitante asignado.
* Los roles RBAC de Azure y los roles de administrador de Entra ID se pueden usar juntos para administrar el acceso tanto a los recursos de Azure como a los recursos de Entra ID.